UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/736,229	12/15/2000	David Giroux	11953.0003	8649

7590 07/12/2004

Stuart T. F. Huang
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, DC 20036

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 07/12/2004

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/736,229	GIROUX ET AL.
	Examiner	Art Unit
	Longbit Chai	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

2. The effective filing date for the subject matter defined in the pending claims in this application is 12/15/2000.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1 – 3, 15 – 18, 22, 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak (Patent Number: US 6289450 B1), hereinafter referred to as Pensak, in view of Okamoto (Patent Number: 6732106), hereinafter referred to as Okamoto.

2. As per claims 1 and 26, Pensak teaches a method of controlling distribution of a segment of encrypted electronic information, comprising:

a. receiving, from a key server, a protected decryption key associated with the segment (Pensak: see for example, Column 8 Line 35 – 45: Pensak teaches receiving the decryption key from the key server associated with the segment. Pensak does not

teach receiving the protected decryption key from the key server associated with the segment).

3. Okamoto teaches receiving the protected decryption key from the key server associated with the segment (Okamoto: see for example, Column 3 Line 55 – 58).

4. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Okamoto within the system of Pensak because (a) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50) and (b) Okamoto provides a method of secure passing of sensitive data between the distribution server and the user device.

5. Pensak as modified further teaches:

b. retrieving, at a user location, the segment (Pensak: see for example, Column 8 Line 35 – 45);

c. obtaining an unprotected copy of the decryption key from the protected decryption key (Okamoto: see for example, Column 3 Line 55 – 58);

d. decrypting, in response to said obtaining, the segment using the unprotected copy of the decryption key (Pensak: see for example, Column 8 Line 39 – 40);

e. destroying the unprotected copy of the decryption key at the user location in response to said decrypting (Pensak: see for example, Column 8 Line 40 – 45);

f. displaying the decrypted segment in response to said decrypting (Pensak: see for example, Column 8 Line 40 – 45); and

g. destroying the decrypted segment in response to said displaying (Pensak: see for example, Column 8 Line 40 – 45).

6. As per claim 15, Pensak teaches a method for controlling distribution of electronic information, comprising:

a. retrieving, at a user location, a segment of encrypted electronic information (Pensak: see for example, Column 8 Line 35 – 45);

7. Pensak does not teach receiving, from a key server, an encrypted decryption key for the segment.

8. Okamoto teaches:

b. receiving, from a key server, an encrypted decryption key for the segment (Okamoto: see for example, Column 3 Line 55 – 58);

9. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Okamoto within the system of Pensak because (a) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50) and (b) Okamoto provides a method of secure passing of sensitive data between the distribution server and the user device.

10. Pensak as modified further teaches:

c. saving said encrypted decryption key in a memory (Okamoto: see for example, Column 3 Line 55 – 58);

d. obtaining a decrypted copy of the decryption key in response to an authorized user request to access the segment (Okamoto: see for example, Column 3 Line 55 – 58) and (Pensak: see for example, Column 8 Line 35 – 45) and;

e. accessing the segment using the decrypted copy of the decryption key at the user location for the segment (Pensak: see for example, Column 8 Line 35 – 45); and

f. destroying the decrypted copy of the decryption key at the user location in response to said accessing without destroying the encrypted decryption key in memory (Pensak: see for example, Column 8 Line 35 – 45).

11. As per claim 17, Pensak teaches a method of accessing a protected segment of electronic information, the segment having an associated key, comprising:

a. retrieving, at the user location, the segment (Pensak: see for example, Column 8 Line 35 – 45);

b. receiving, at the user location from the remote server, the key (Pensak: see for example, Column 8 Line 35 – 45);

c. accessing the segment, in response to said receiving, using the key (Pensak: see for example, Column 8 Line 35 – 45);

d. displaying the segment as accessed (Pensak: see for example, Column 8 Line 35 – 45);

e. destroying the key in response to one of said displaying and said accessing, wherein the key is never stored in memory at a user location between said receiving and said destroying (Pensak: see for example, Column 8 Line 35 – 45);

12. Pensak does not teach receiving, at the user location from the remote server, an encrypted key lease including the key.

13. Okamoto teaches:

f. receiving, at the user location from the remote server, an encrypted key lease including the key (Okamoto: see for example, Column 3 Line 55 – 58);

14. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yaegashi within the system of Pensak because (a) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50) and (b) Okamoto provides a method of secure passing of sensitive data between the distribution server and the user device.

15. Pensak as modified further teaches:

g. saving the encrypted key lease in a memory (Okamoto: see for example, Column 3 Line 55 – 58);

h. breaking a connection between the user location and the remote server; and during a period of the broken connection: retrieving, at the user location, the segment (Pensak: see for example, Figure 2 Element 1056 / 1058, Element 1064 / 1066: The

Figure 2 clearly discloses that the session connection of SSL layer would be over (i.e. broken) after receiving the decryption key from the server to allow the next request for a new session connection to use a new server random number as the second information to encrypt the decryption key. Subsequently, the segment is then displayed and viewed at the user view tool as the result of successful receiving the decryption key).

j. obtaining a decrypted copy of the key from the key lease (Okamoto: see for example, Column 3 Line 55 – 58) and (Pensak: see for example, Column 8 Line 35 – 45);

k. accessing the segment in response to said obtaining (Pensak: see for example, Column 8 Line 35 – 45);

l. displaying the segment as accessed (Pensak: see for example, Column 8 Line 35 – 45); and

m. destroying the decrypted copy of the key in response to one of said displaying and said accessing (Pensak: see for example, Column 8 Line 35 – 45).

16. As per claim 22, Pensak teaches a method of viewing a segment of encrypted electronic information on a display, comprising:

a. receiving, from a remote server, an encrypted decryption key for the segment (Pensak: see for example, Column 8 Line 35 – 45: Pensak teaches receiving the decryption key from the key server associated with the segment. Pensak does not teach receiving the protected decryption key from the key server associated with the segment).

17. Okamoto teaches receiving an encrypted decryption key for the segment (Okamoto: see for example, Column 3 Line 55 – 58).

18. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Okamoto within the system of Pensak because (a) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50) and (b) Okamoto provides a method of secure passing of sensitive data between the distribution server and the user device.

19. Pensak as modified further teaches:

b. retrieving, at a user location, a segment of encrypted electronic information (Okamoto: see for example, Column 3 Line 55 – 58) and (Pensak: see for example, Column 8 Line 35 – 45);

c. first decrypting the encrypted decryption key in response to the presence of authorized conditions (Okamoto: see for example, Column 3 Line 55 – 58) and (Pensak: see for example, Column 8 Line 35 – 45);

d. second decrypting the segment using the decrypted decryption key (Pensak: see for example, Column 8 Line 35 – 45);

e. destroying, at the user location, all copies of the decrypted decryption key in response to said second decrypting, without destroying the encrypted decryption key (Pensak: see for example, Column 8 Line 35 – 45);

f. displaying the segment as decrypted on the display (Pensak: see for example, Column 8 Line 40 – 45); and

g. destroying, at the user location, the segment as decrypted in response to said displaying (Pensak: see for example, Column 8 Line 40 – 45).

20. As per claim 2 and 27, Pensak as modified teaches the claimed invention as described above (see claim 1 and 26). Pensak as modified further teaches saving, in response to said receiving, the protected decryption key; wherein said destroying the unprotected copy of the decryption key does not effect the unprotected copy of the decryption key (Okamoto: see for example, Column 3 Line 55 – 58).

21. As per claim 3, Pensak as modified teaches the claimed invention as described above (see claim 1). Pensak as modified further teaches said receiving further comprising receiving at least one access policy associated with at least one of the key server, the user location, the segment, the decryption key, and a user, the at least one access policy including at least one fixed time limitation; said determining comprising determining whether current operating conditions, including the current time, satisfy the at least one access policy (Pensak: see for example, Column 6 Line 36 – 43 and Column 5 Line 55 – 58).

22. As per claim 16, Pensak as modified teaches the claimed invention as described above (see claim 15). Pensak as modified further teaches displaying the decrypted segment in response to said accessing; and destroying the decrypted segment in response to one of said displaying (Pensak: see for example, Column 8 Line 40 – 45).

23. As per claim 18, Pensak as modified teaches the claimed invention as described above (see claim 17). Pensak as modified further teaches restoring a connection between the user location and the remote server (Pensak: see for example, Figure 2 Element 1056 / 1058, Element 1064 / 1066: The Figure 2 clearly discloses that the session connection of SSL layer would be over (i.e. broken) after receiving the decryption key from the server to allow the next request for a new session connection to use a new server random number as the second information to encrypt the decryption key. As a result, the session need to be re-established and the connection between the user location and the remote server need to be restored.

24. Claims 5 – 7, 9, 19, 21, 24 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak (Patent Number: US 6289450 B1), hereinafter referred to as Pensak, in view of Yaegashi (Patent Number: US 6499106 B1), hereinafter referred to as Yaegashi.

25. As per claim 5, Pensak teaches a method for issuing a key lease, comprising:

a. receiving, at a remote server, a request to lease a decryption key for an encrypted electronic segment (Pensak: see for example, Column 3 Line 23 – 25);

b. determining whether a key lease can be issued for the encrypted electronic information based on at least one of a remote server restriction, an information restriction, and a user restriction (Pensak: see for example, Column 6 Line 37 – 44);

26. Pensak teaches the server creating a voucher as a copy of a descryption key and at least one user limitation associated with the decryption key (Pensak: see for example, Column 9 Line 37 – 40).

27. Pensak does not expressly teach voucher including at least one time limitation associated with the decryption key.

28. Yaegashi teaches:

c. creating a voucher in response to a determination that the key lease can be issued, said voucher including at least the decryption key, and at least one time limitation associated with the decryption key (Yaegashi: see for example, Column 12 Line 19 – 28: Yaegashi discloses a key expiration security mechanism to use the decryption key. This time expiration security mechanism is implementation at the information access system; but, however, it is dictated by the central access control system (i.e. the server) as mostly understood in the field).

29. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yaegashi within the system of Pensak because (a) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50) and (b) Yaegashi discloses a secure method for information distribution and especially for storing and transferring encrypted data to

remote destinations and a security agent to provide access to the data (Yaegashi: see for example, Column 1 Line 8 – 13).

30. Pensak as modified further teaches:

d. encrypting at least the decryption key of the voucher; and sending the voucher to the user location (Yaegashi: see for example, Column 12 Line 50 – 51).

31. As per claim 24, Pensak teaches a method of limiting access to a segment of encrypted information, comprising:

a. saving, at a remote server, a decryption key for the segment, the segment being at a location other than the remote server (Pensak: see for example, Column 2 Line 44 – 57);

b. receiving a request from an authorized user for the decryption key (Pensak: see for example, Column 8 Line 26 – 34);

c. sending a copy of the decryption key from the remote server to a source of the request (Pensak: see for example, Column 8 Line 34 – 46);

32. Pensak does not teach destroying the decryption key at the remote server in response to the elapse of a predetermined period of time.

33. Yaegashi teaches:

d. destroying the decryption key at the remote server in response to the elapse of a predetermined period of time (Yaegashi: see for example, Column 12 Line 19 – 28: Yaegashi discloses a key expiration security mechanism to use the decryption key.

This time expiration security mechanism is implementation at the information access system; but, however, it is dictated by the central access control system (i.e. the server) as mostly understood in the field).

34. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yaegashi within the system of Pensak because (a) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50) and (b) Yaegashi discloses a secure method for information distribution and especially for storing and transferring encrypted data to remote destinations and a security agent to provide access to the data (Yaegashi: see for example, Column 1 Line 8 – 13).

35. As per claim 6, Pensak as modified teaches the claimed invention as described above (see claim 5). Pensak as modified further teaches said creating further comprises adding access policies associated with the information to the voucher (Pensak: see for example, (Pensak: see for example, Column 6 Line 36 – 43 and Column 5 Line 55 – 58).

36. As per claim 7, Pensak as modified teaches the claimed invention as described above (see claim 5). Pensak as modified further teaches said receiving further comprises receiving a requested time frame of use of the key lease, and wherein the at

least one time limitation includes an expiration time based on at least one of a maximum allowed by the remote server, a maximum allowed by the information, a maximum allowed by user limitations, and the requested time frame (Yaegashi: see for example, Column 12 Line 19 – 26).

37. As per claim 9, Pensak as modified teaches the claimed invention as described above (see claim 5). Pensak as modified further teaches destroying the decryption key at the remote server after a predetermined period of time (Yaegashi: see for example, Column 12 Line 19 – 26).

38. As per claim 19, Pensak as modified teaches the claimed invention as described above (see claim 18). Pensak as modified does not teach revoking the key lease after said restoring.

39. Yaegashi teaches revoking the key lease after said restoring (Yaegashi: see for example, Column 12 Line 25: Yaegashi teaches, under the policy of key expiration security mechanism, the key should be immediately expired as soon as an invalid attempt to access stored keys is detected).

40. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yaegashi within the system of Pensak because (a) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50) and (b) Yaegashi discloses a secure method for

information distribution and especially for storing and transferring encrypted data to remote destinations and a security agent to provide access to the data (Yaegashi: see for example, Column 1 Line 8 – 13).

41. As per claim 21, Pensak as modified teaches the claimed invention as described above (see claim 20). Pensak as modified does not teach detecting, at one of the user location and the remote server, from the contents of the log, any tampering at the user location relating to at least one of the key lease, the segment, and operating conditions at the user location.

42. Yaegashi teaches detecting, at one of the user location and the remote server, from the contents of the log, any tampering at the user location relating to at least one of the key lease, the segment, and operating conditions at the user location (Yaegashi: see for example, Column 12 Line 25: Yaegashi teaches any tampering at the user location relating to at least one of the key lease should be detected because, under the policy of key expiration security mechanism, the key must be immediately expired as soon as an invalid attempt to access stored keys is detected).

43. Same rationale of combination applies here as above in rejecting the claim 19.

44. As per claim 25, Pensak as modified teaches the claimed invention as described above (see claim 24). Pensak as modified further teaches preventing the source from storing the copy of the decryption key, wherein said destroying leaves said segment permanently inaccessible absent breaking of the encryption protecting of the segment (Pensak: see for example, Column 8 Line 40 – 45).

45. Claims 12 – 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak (Patent Number: US 6289450 B1), hereinafter referred to as Pensak, in view of Chen (Patent Number: US 6182220 B1), hereinafter referred to as Chen.

46. As per claim 12, Pensak teaches a method of controlling distribution of electronic information, comprising:

a. sending, from a user location to a key server, a request to access a protected segment, and a first information (Pensak: see for example, Column 8 Line 26 – 34);

47. Pensak does not teach receiving, at the user location from the key server, an encrypted voucher and a second information.

48. Chen teaches:

b. receiving, at the user location from the key server, an encrypted voucher and a second information, said voucher including at least a decryption key associated with the segment (Chen: see for example, Column 3 Line 48 – 50: Chen teaches the following concepts. The first information sender sends the first information (a client random seed) to the first information receiver. The first information receiver then sends the second information (a server random seed) to the first information sender. The first information sender then uses the combination of the first information and the second information to encrypt the sensitive data of interest (password) and then sends the protected sensitive data to the first information receiver);

49. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Chen within the system of Pensak

because because (a) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50) and (b) Chen teaches an enhanced secure method to protect the sensitive data regarding the privacy issue (Chen: see for example, Column 1 Line 52 – 55). The type of sensitive data context to be protected is obviously insignificant since the problem to be addressed and resolved is the privacy issue on security regards. The combination of the first information and the second information is used to derive the DES encryption key so that the security risk to intercept both of the first information and the second information can be significantly reduced.

50. Pensak as modified further teaches:

c. retrieving, at a user location, the segment (Pensak: see for example, Column 8 Line 35 – 45);

d. obtaining a decrypted copy of the decryption key using the first and second information (Chen: see for example, see for example, Column 3 Line 48 – 50);

e. accessing, in response to said decrypting, the segment using the at least a portion of the voucher (Pensak: see for example, Column 8 Line 35 – 45);

f. destroying, in response to said accessing, the decrypted copy of the decryption key (Pensak: see for example, Column 8 Line 35 – 45).

51. As per claim 13, Pensak as modified teaches the claimed invention as described above (see claim 12). Pensak as modified further teaches displaying the accessed segment in response to said accessing; and destroying the accessed segment in response to said displaying (Pensak: see for example, Column 8 Line 40 – 45).

52. As per claim 14, Pensak as modified teaches the claimed invention as described above (see claim 12). Pensak as modified further teaches determining, in response to said decrypting, whether operating parameters satisfy the access policies; and said accessing being responsive to said operating parameters being determined to satisfy the access policies; wherein said accessing is responsive to said decrypting through said determining (Pensak: see for example, Column 6 Line 36 – 43 and Column 5 Line 55 – 58).

53. Claims 10 – 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak (Patent Number: US 6289450 B1), hereinafter referred to as Pensak, in view of Chen (Patent Number: US 6182220 B1), hereinafter referred to as Chen, and in view of Chen-2 (Patent Number: 5822524), hereinafter referred to as Chen-2.

54. As per claim 10, Pensak as modified teaches the claimed invention as described above (see claim 5). Pensak as modified does not teach logging said obtaining in a log; and sending, from the user location to a remote server, the log.

55. Chen-e teaches:

56. logging said obtaining in a log; and sending, from the user location to a remote server, the log (Chen-2: see for example, Column 11 Line 21 – 23).

57. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Chen-2 within the system of Pensak as modified because (a) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50) and (b) Chen-2 teaches methods for retrieval of multimedia files over distributed systems and networks (Chen-2: see for example, Column 1 Line 9 – 10).

58. As per claim 11, Pensak as modified teaches the claimed invention as described above (see claim 10). Pensak as modified further teaches comprising logging a time of said obtaining in the log (Chen-2: see for example, Column 11 Line 21 – 23).

59. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak (Patent Number: US 6289450 B1), hereinafter referred to as Pensak, in view of Okamoto (Patent Number: 6732106), hereinafter referred to as Okamoto and in view of Chen-2 (Patent Number: 5822524), hereinafter referred to as Chen-2.

60. As per claim 20, Pensak as modified teaches the claimed invention as described above (see claim 18). Pensak as modified does not teach logging said obtaining in a

log; and sending, after said restoring, the log from the user location to the remote server.

61. Chen-2 teaches:

62. logging said obtaining in a log; and sending, after said restoring, the log from the user location to the remote server.

63. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Chen-2 within the system of Pensak as modified because (a) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50) and (b) Chen-2 teaches methods for retrieval of multimedia files over distributed systems and networks (Chen-2: see for example, Column 1 Line 9 – 10).

64. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak (Patent Number: US 6289450 B1), hereinafter referred to as Pensak, in view of Yaegashi (Patent Number: US 6499106 B1), hereinafter referred to as Yaegashi and in view of Chen (Patent Number: US 6182220 B1), hereinafter referred to as Chen.

65. As per claim 8, Pensak as modified teaches the claimed invention as described above (see claim 5). Pensak as modified does not teach said encrypting utilizing a first

information from the user location and a second information from the remote server; and said sending further comprises sending the second information to the user location; wherein the second information is insufficient in and of itself to decrypt the voucher.

66. Chen teaches:

67. said encrypting utilizing a first information from the user location and a second information from the remote server; and said sending further comprises sending the second information to the user location; wherein the second information is insufficient in and of itself to decrypt the voucher.

68. See the same rationale applies here as above in rejecting the claim 12.

69. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yaegashi (Patent Number: US 6499106 B1), hereinafter referred to as Yaegashi, in view of Pensak (Patent Number: US 6289450 B1), hereinafter referred to as Pensak, in view of Jevans (Publication Number: US 2001/0055396 A1), hereinafter referred to as Jevans.

70. As per claim 23, Yaegashi teaches a method of controlling distribution of a segment of encrypted electronic information, the segment having a first and second portion, the method comprising:

a. receiving, from a key server, an encrypted voucher, the voucher including first and second decryption keys associated with the first and second portions, respectively (Yaegashi: see for example, Column 12 Line 50 – 55: Yaegashi teaches receiving, from

a key server, an encrypted voucher. But, Yaegashi does not teach the voucher including first and second decryption keys associated with the first and second portions, respectively.

71. Jevans teaches the voucher including first and second decryption keys associated with the first and second portions, respectively (Jevans: see for example, Paragraph [0021] Line 9 – 12 and Paragraph [0024]: Jevans teaches the encrypted descrytion keys could be bundled into the message without compromising the security of the mechanism).

72. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Jevans within the system of Yaegash because the communication efficiency can be improved by implementing the concatenation on a list of decryption keys associated with a list of requested segments within the same packet by reducing the number of exchanged messages between the server and the client.

73. Yaegash as modified further teaches:

b. retrieving, at a user location, the segment (Yaegash: see for example, Figure 3 Step 15 S15);

c. accessing the protected copy of the first decryption key (Yaegashi: see for example, Column 12 Line 29 – 56);

d. decrypting, in response to said accessing, the first portion of the segment using the accessed copy of the first decryption key (Yaegashi: see for example, Column 12 Line 29 – 56);

74. Yaegash as modified does not teach destroying the accessed copy of the first decryption key at the user location in response to said decrypting.

75. Pensak teaches:

e. destroying the accessed copy of the first decryption key at the user location in response to said decrypting (Pensak: see for example, Column 8 Line 40 – 45);

76. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Pensak within the system of Yaegashi as modified as modifed because (a) Yaegashi discloses a secure method for information distribution and especially for storing and transferring encrypted data to remote destinations and a security agent to provide access to the data (Yaegashi: see for example, Column 1 Line 8 – 13) and (b) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50).

77. Yaegash as modified further teaches:

f. displaying the decrypted segment in response to one of said decrypting and said destroying (Pensak: see for example, Column 8 Line 40 – 45);

g. destroying the decrypted first portion in response to said displaying (Pensak: see for example, Column 8 Line 40 – 45);

h. accessing the protected copy of the second decryption key after said destroying the first decrypted segment (Pensak: see for example, Column 8 Line 44 – 46); and

i. decrypting, in response to said accessing the protected copy of the second decryption key, the second portion of the segment using the accessed copy of the second decryption key (Pensak: see for example, Column 8 Line 44 – 46).

78. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak (Patent Number: US-6289450 B1), hereinafter referred to as Pensak, in view of Okamoto (Patent Number: 6732106), hereinafter referred to as Okamoto, and in view of Yaegashi (Patent Number: US 6499106 B1), hereinafter referred to as Yaegashi.

79. As per claim 4, Pensak as modified teaches the claimed invention as described above (see claim 1). Pensak as modified does not teach further teaches saving, in response to said receiving, the protected decryption key in memory; and rendering the protected copy of the decryption key inaccessible after an expiration time in the at least one access policy.

80. Okamoto teaches:

a. saving, in response to said receiving, the protected decryption key in memory (Okamoto: see for example, Column 3 Line 55 – 58).

81. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Okamoto within the system of Pensak because (a) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the

electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50) and (b) Okamoto provides a method of secure passing of sensitive data between the distribution server and the user device.

82. Pensak as modified does not teach rendering the protected copy of the decryption key inaccessible after an expiration time in the at least one access policy.

83. Yaegashi teaches:

b. rendering the protected copy of the decryption key inaccessible after an expiration time in the at least one access policy (Yaegashi: see for example, Column 12 Line 19 – 26).

84. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yaegashi within the system of Pensak as modifiied because (a) Pensak discloses a system and method for encrypting electronic information so that access the information can be controlled by the author or other controlling party as well as the method that a central server maintains control over the electronic encryption and decryption keys used by the remote user station (Pensak: see for example, Column 1 Line 29 – 50) and (b) Yaegashi discloses a secure method for information distribution and especially for storing and transferring encrypted data to remote destinations and a security agent to provide access to the data (Yaegashi: see for example, Column 1 Line 8 – 13).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100